SECURITY

Staying Ahead of the Hack: Operationalizing Threat Intelligence to Strengthen Defenses

Many pieces of forensic evidence come into play when investigating a crime scene – analysis of fingerprints, DNA, shoe prints, videos/photos, ballistics, etc. By analyzing the data, a picture of the crime emerges, which in the case of a serial killer often includes his or her MO or method of operation.
In the cyber world, analysts do the same thing.

They analyze indicators of compromise (IoCs) or observables as they are often called – IPs, domains, URLs, hashes, etc. Pieces of information that describe an incident that has already happened. Many cyber criminals reuse tactics and techniques that produce the same observables and therefore create a pattern that can be used to detect and prevent future attacks by the same actors.

Many analysts extract the observables from the investigation to create blacklists or pattern-based signatures containing hundreds of observables of the same type, however, these “simple” lists are prone to false positives and can generate volumes of generic threat alerts.

These must be manually reviewed and can overwhelm security teams, putting effective security at risk.
So in order to sift through the massive data to better identify and stop threats, the cyber security industry has focused more and more on developing improved cyber threat intelligence. Today cyber threat intelligence is everywhere thanks to efforts to augment sharing through open standards for threat intelligence like STIX and TAXII and a variety of threat intelligence vendors. Nevertheless, making use of threat intelligence from multiple sources can be time intensive and complicated without

the right tools.
But imagine this…

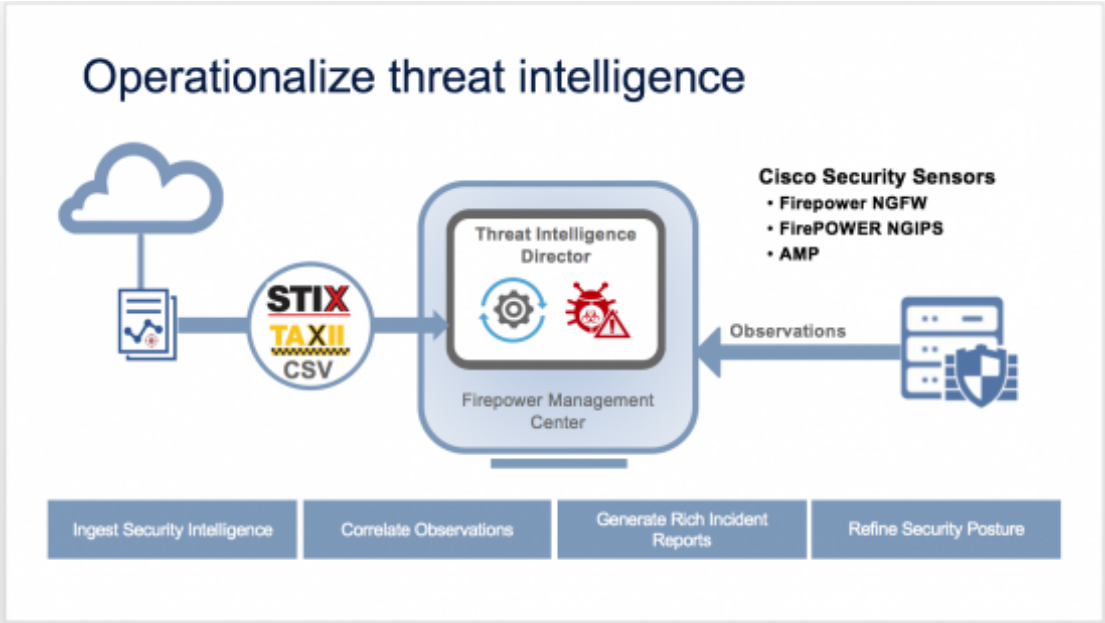
You receive intelligence from an industry sharing group like FS-ISAC warning you of a new attack targeting financial institutions. Several organizations have already been hit and because they didn't have protection in place, they are having to go through an expensive incident response process. Those organizations have shared critical IoCs via FS-ISAC's TAXII feed.

Based on the warning, your team can review the indicators and increase the response on your network sensors from "monitor" to "block." Within hours your organization is targeted but because of the extra intelligence and the ability to automatically block, you stop the attack before it can cause any damage.

Well, you don't have to imagine it. You're able to do this today with a new set of capabilities now built-in to your Firepower Management Center.

Improve Your Security Posture with Threat Intelligence from Multiple Sources
The new Threat Intelligence Director operationalizes cyber threat intelligence in Firepower next-generation firewalls and intrusion prevention systems. By leveraging open industry standards such as STIX and TAXII or simple delineated ASCII, the Intelligence Director can easily ingest third-party threat feeds and data from Threat Intelligence Platforms (TIPs) to your network sensors and next-generation firewalls. Based on your confidence in this additional intelligence, you can direct your network sensors to use it to automatically monitor or block traffic inline.

Confirmed incidents are published from Cisco Firepower sensors to your Firepower Management Center so you have better visibility into attacks against your network.



Save Time and Stop Adversaries in their Tracks
Threat Intelligence Director reduces the time you might have spent manually copying and pasting observables from intelligence reports into sensor-specific blacklists or chasing down the right piece of intelligence with context related to a generic alert.

Working with your sensors, it confirms and correlates events across multiple devices, matches against indicators, and creates incidents with all your contextual data in one place. Security operations can make faster, more informed decisions on the right course of action.

I know I have hit this theme repeatedly but I cannot resist pointing out that the Threat Intelligence Director is yet another example of how Cisco is making security more effective with solutions that are simple, open, and automated. It is also an excellent example of what “actionable intelligence” is all about – enhancing your ability to rapidly and accurately analyze and respond to security threats.

Intelligence analysts in both law enforcement and cyber security, use similar techniques to identify and prevent serialized crime and campaigns. With Threat Intelligence Director and Cisco's Firepower devices you have the best technology to leverage intelligence and to stop adversaries in their tracks.

This article was originally done by - Jason Lamar – Cisco